Date	FMV Document ID	Issue
2008-09-30	43827/2008	1.0
	Unit	Subject Code
	MNE 5, Swe Tech Team	
Document responsible	Assignment ID	Reference ID	Page
Mats Ericsson, FMVMats Ericsson, FMV	MNE5 IEAT	LT7O E08-0429	1 (22)

Approved by/Role	Document status
	Final MNE 5 product

Information Exchange Architecture and Technology Concept in the MNE5 environment

Summary

A comprehensive approach to operations is today one of the cornerstones to engagement in conflict areas. Interagency collaboration, simultaneous and coordinated use of both military and civilian means to solve critical problems is desired. This increases demands on all participating organisations and their technical systems to share and exchange information over previous borders. The Information Exchange Architecture and Technology (IEAT) Concept, based upon the Swedish Armed Forces Network Based Defence (NBD) program, describes how exchange of information can be performed in a way that meets the operational requirements in a *comprehensive response operation*. It articulates principles for information exchange as well as supporting architecture and possible technologies.

Comprehensive Approach is a concept which builds upon the principle of collaboration between all participating actors in an operation. To ensure effectiveness, exchange of information between various organisations must be organised and prepared. The IEAT Concept sets the scene for this.

Some key principles for the IEAT Concept are sovereignty of collaboration actors and a view on information as an operation wide asset. Formal agreements between nations are required for information sharing and the concept of Service Oriented Architecture is a foundation for the IEAT Concept.

Implementation of any concept is based upon understanding and acceptance. The IEAT Concept covers the policy environment at highest national decision level and it also describes plausible techniques down to technical details. It is not possible to start implementation at the same time as an operation is planned, therefore the IEAT Concept must be implemented during normal routine activities within a nation or organisation.

Following the principles in the IEAT Concept, an environment can be built were information exchange is effective and flexible enough to support a *comprehensive response operation*.

Distributed:
Date:

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
30 SEP 2008	**Final**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Exchange Architecture and Technology Concept in the MNE5 Environment	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Mats Ericsson	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Swedish Defence Materiel Administration (Försvarets materielverk, FMV), Stockholm, Sweden	**43827/2008**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
USJFCOM J9 Joint Concept Development and Experimentation, Suffolk, VA	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT
The Information Exchange Architecture and Technology (IEAT) Concept, based upon the Swedish Armed Forces Network Based Defence (NBD) program (which is based upon a Service Oriented Architecture (SOA) approach) describes how exchange of information can be performed in a way that meets the operational requirements in a comprehensive response operation. It articulates principles for information exchange as well as supporting architecture and possible technologies.

15. SUBJECT TERMS
multinational, experiment, MNE, information exchange, service oriented architecture, network centric, collaboration,

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**22**	

Table of content

1 INTRODUCTION 3

1.1 PURPOSE 3
1.2 BACKGROUND 3
1.3 ASSUMPTIONS, BASED ON MNE5 REQUIREMENT 3
1.4 SCOPE 4
1.5 LIMITATIONS 4
1.6 REFERENCES 4

2 DRIVERS FOR CHANGE 5

3 CHALLENGES 5

4 POSITIONING OF THE IEAT CONCEPT 7

5 DESCRIPTION OF THE IEAT CONCEPT 9

5.1 KEY PRINCIPLES 10
5.2 INFORMATION EXCHANGE 11
5.3 ARCHITECTURE 12
5.4 SECURITY 18

6 ESTABLISHMENT AND USE OF THE IEAT CONCEPT 20

6.1 UNDERSTAND, ACCEPT AND CHANGE ATTITUDE 20
6.2 PARTICIPATION AND ACCEPTANCE OF SHARING INFORMATION 20
6.3 ESTABLISH THE "PHYSICAL" PLAYGROUND FOR INFORMATION EXCHANGE 21
6.4 ESTABLISH THE "LOGICAL" PLAYGROUND FOR INFORMATION EXCHANGE 21
6.5 BEFORE AND DURING AN INTERNATIONAL OPERATION 22
6.6 FEEDING BACK TO THE BIGGER LOOP, DEVELOPING THE IEAT CONCEPT 22

1 Introduction

1.1 Purpose

This paper articulates the Information Exchange Architecture Technology (IEAT) Concept.

The purpose of the IEAT Concept is to improve exchange of information in MNE5 and other similar environments.

The IEAT Concept is developed from The Swedish Armed Forces Network Based Defence (NBD) program which is based upon a Service Oriented Architecture (SOA) approach.

1.2 Background

The development in the society the last years, and what seems to be a trend for the coming years, has a great impact on military actions and required capabilities. The speed in which changes occur is far greater than before. New and different threats explode in unexpected geographical places and require quicker and more flexible capabilities than ever before. Politically changes seems to follow the same pace, political leaders are challenged to engage and commit more decisive and in more conflict areas. Coalitions of nations are put together more frequently than before even if static organisations normally play the main role. A comprehensive approach to engagement in conflicts is one of the cornerstones today. Interagency collaboration and coordinated use of both civil and military means to solve situations provide better effectiveness. This increases the requirements on all participants' operational and technical systems' ability to exchange information over previous borders. Conventional military systems do neither have enough ability to exchange information to actors outside the military environment nor the flexibility needed to deal with the rapidly changing global environment.

The means to meet these new requirements come from another major development in the last decade: the information technology revolution, and particularly the advances in network and telecommunications technology. The IEAT Concept is focused on taking advantage of civilian technology, using COTS as much as possible in suggested solutions. The civilian development, Service Oriented Architecture (SOA) is one of the cornerstones in the IEAT Concept.

1.3 Assumptions, based on MNE5 requirement

The IEAT Concept is intended to be used in joint peace supporting missions, crisis situations or similar operations where there is a centrally led approach, coordinating the objectives and activities of Defence, Government Organizations, Non-Government Organizations and coalition partners. Even though an operation is centrally led all the participating parties are not necessarily in command from a central office.

A participating party has its own sovereignty.

The success of an operation is depended on collaborative working and information sharing among the parties, enabling superior risk assessment and decision making.

An operation could be either national or international.

In this paper an operation following this approach will be called a *comprehensive response operation*.

1.4 Scope

The IEAT Concept describes and provides guidelines on how exchange of information can be conducted in Information Technology systems to support the principals of Comprehensive Approach and interagency cooperation.

The IEAT Concept cover information exchange agreements including information exchange models, information exchange requirements, translations, semantic areas clustering fielded system of system services and instruments for data exchange.

The IEAT Concept also outlines architecture to support information exchange. The Concept defines the technical and organizational elements including how these elements shall communicate with each other and which standards they shall follow.

In order to make the architecture consistent and understandable by all involved parties in a *comprehensive response operation* an architecture description framework is included. This description framework defines how the technical and organizational elements shall be described and explains how the descriptions shall be interpreted.

The IEAT Concept also identifies and describes a set of core technologies which are needed to implement the Concept. This includes technologies for finding and connecting to other parties' technical systems in a secure way, collaboration technologies to enable human to human interaction and federated registries for finding persons and information in other parties' technical systems.

1.5 Limitations

The IEAT Concept does not describe organizational structures, methods or doctrines for interoperability. However, these have a direct impact on the IEAT Concept implementation since they set requirements for information exchange between organizations.

1.6 References

The IEAT Concept is based upon findings during Swedish national development of a network enabling capability. Document that describes the results of this work and conclusions are to be found at www.fmv.se.

2 Drivers for change

A comprehensive approach to a situation has to deal with complex environments were both national and international actors must operate efficiently together. Interoperability between organizational structures, methods and technical systems is therefore absolutely crucial. National information becomes international, military information may be used by governmental and other non-governmental organizations.

Changing operational environment requires new principles of cooperation. Yesterdays pre-arranged organisations with mainly fixed structures and technical systems do not support the new situation efficiently enough. The political desire to organise ad-hoc formations within short timeframes puts new demands on most areas. Any organisation or actor today needs the capability to provide parts of its information to others as well as having the ability to use information from external sources to a much larger extent than before. Even though collaborating parties is optimized for information dissemination within its own organization, they now must have the capability to disseminate and exchange information beyond previous borders.

Doctrinal and conceptual development today clearly outlines that multi-use of information will cross both between command levels and between different functions

The level of collaboration will naturally be based upon the specific mission, where both organisations and technical systems must have flexibility enough for a smooth and quick adoption to new configurations.

However, current techniques of collaboration like:

- regular mail and fax, electronic mail (secure and unsecured),
- file transfer via various types of media, e.g. diskettes, portable discs, memory sticks, electronic file transfer via a network connection,
- single system approach, point-to-point integrations or other IT systems that need to exchange information without any reflections on re-use after a specific operation.

do not provide adequate effect to meet the requirements of information exchange in a *comprehensive response operation*. A new approach for information exchange underpinned by architecture and technology is therefore required.

3 Challenges

In a perfect world Information Exchange would be part of Information Management covering integrated management processes, procedures and services that enable all parties to store, locate, retrieve and transmit information between all parties involved. Appropriate information would be presented in a form and quantity adjustable and suitable for every situation.

However, the world isn't perfect. It is not likely that there will be an all encompassing Information Management in place in a *comprehensive response operation*. Reaching Information Exchange to a level that supports and enables superior risk assessment and decision making includes several challenges.

Challenges based on international agreements and regulations

Information exchange between states (e.g. unclassified, restricted, secret and top secret classification) is based on government agreement between states. Qualified information exchange could not take place if such agreement does not exist. To achieve an agreement we are looking at a process that generally takes many months up to a year or more. It has also been proven complicated to negotiate and sign such agreement between more than two states at a time (multilateral). Nations are willing to share more information with some parties and less with others. This creates complicated situations during multilateral operations. This becomes even more complicated when involving government authorities other than the military.

In this perspective technical issues are only one part of the problem.

Challenges based on national law, national integrity and regulations

Differing laws, rules and regulations together with different cultures regarding information sharing are likely to impact willingness to share information and slow down process of getting agreements on what to share.

Participating parties are likely to have different requirements and priorities which will imply different scope and granularity of information exchange for each party.

Participating parties are likely to wish to get access to more information than they are willing to provide themselves.

Lack of understanding of capabilities, limitations and culture of other collaborating parties may decrease the desire to explore new opportunities of collaboration and thereby impact the information exchange needs.

Even within each country this kind of problems may occur.

Challenges based on interpretation of information content

Semantic differences are likely to be an issue when exchanging information.

Trust of accessible information will be challenged, it will set high demands on the ability to verify the source and to guarantee integrity of information.

The content of information exchanged between different systems/actors must be sufficiently known so that requirements for such exchange of information can be agreed upon The ability to rapidly change directions of the flow of information, as well as the actual content is one basis for information exchange.

Any formation of operational groupings must appreciate differences in requirements and goals. Different approaches on the way towards an end-state must eventually meet in a combined opinion, a common and agreed set of descriptions on how to reach wanted effects.

Trust of accessible information is essential, secure and assured information must always be maintained.

Challenges based on technical issues

Huge amounts of data of various kinds will exist in a large number of technical information systems requiring means to organize and prioritize what to share.

The sovereignty of the parties will increase the complexity of agreeing on standards and formats for information exchange since there is no governing organ that can make the decisions.

Architecture and technical implementations of information systems will be different in most of the cases.

The complete technical system will probably not be homogenous, rather a federation of heterogeneous systems and therefore hard to govern and manage.

The usage and maturity of using architecture and design as governing tools is likely to vary greatly among collaborating parties, thus slowing down the process of getting a common understanding and agreement on the architecture.

Challenges based on lack of trust, mental block and organizational issues

Generally we tend to hesitate to share ("give away") information to other parties. Even if we have solved "challenges based on international agreements and regulations" we will still most likely hesitate to share information. This is understandable, but not very efficient from an operational perspective. We have to overcome these limitations and see the goal of the operations as more important than the individual organisations ego.

Today's military organizations are experienced and usually organized around various stovepipe principles. This is a convenient, straight forward way of defining requirements, responsibilities and timetables for implementing new and enhanced systems. A *comprehensive response operation*, were information is expected to be exchanged between both organisations and technical systems, will set new requirements on the procurement process, working methods and the organisations working those issues.

4 Positioning of the IEAT Concept

Value Proposition

The IEAT Concept leads to positive effects during the whole life-cycle of an operation, especially when preparing and performing an operation.

- Better effect locally within an area of operations. Participant's situation awareness will increase with access to larger amount of information and the decision cycle can be quicker as a consequence of multiple sources of information.
- Easier and quicker to organise mission specific, or ad-hoc, units/formations at all levels as well as re-organise units during the operation. Organisations may use their normal tools and

systems, when defining, producing and consuming services. The IEAT Concept does not require common systems.

- Possibility for a more efficient acquisition process leading to faster implementation of systems. Defined mechanisms for information exchange also support a more effective life cycle management of systems.

The IEAT Concept also provides significant value to a Network Centric approach by describing principles for efficient information exchange between different systems, processes and concepts.

By providing guidance for how to achieve efficient information flow the IEAT Concept supports critical properties like flexibility, mobility, interoperability, modularity and scalability.

Finally, the IEAT Concept will enable collaborating parties in a *comprehensive response operation* to keep their sovereignty and still provide, and receive, substantial value by sharing own information and consuming other's.

Perspective

As stated in chapter 2, there are many alternative and complementary approaches on how to handle information exchange in a *comprehensive response operation*. All of the previously mentioned means for information exchange are likely to be used in various combinations and to be used for a long time.

However, in the IEAT Concept publication of information provisioning services on a common arena is the main mean of sharing information. A participating actor can consume these services, if authorized to use a particular service. The requirements of services will guide availability of them and when a service no longer is needed by anyone it may be closed if so directed by the parties. It is essential that the stakeholders define their requirements on information exchange and that requirements on services are commonly defined.

Key Stakeholders

The IEAT Concept targets any organization that plan or foresee that it will participate in a collaboration type of mission where exchange of information is vital.

In order to reach a common understanding of the basic principles for information exchange, concept development in areas where information exchange plays an important role should build upon the IEAT Concept. Consequently, authorities tasked to organise crisis response forces at high readiness, both military and civil, as well as various rescue organisations are stakeholders.

5 Description of the IEAT Concept

There are many challenges that have to be overcome in order to make successful collaborative work and information sharing among the actors in an operation successful. The IEAT Concept description addresses these challenges, but focuses mainly on the parts necessary to establish an arena in which collaborating actors can exchange information.

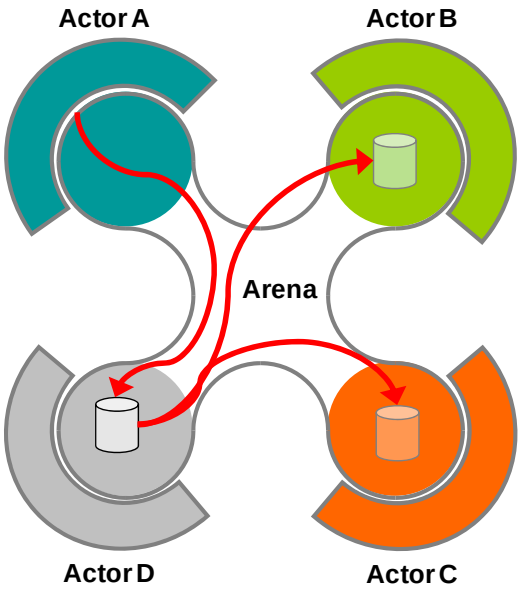

Figure 1 : Collaboration in a Comprehensive response operation environment

In this arena, see Figure 1, the collaborating actors provide services which the other actors can use to enable information exchange.

The actors in the arena will be of different type; military, government, international organisations and non-governmental organisations. These actors may also have different roles in the arena depending on their role in the overall *comprehensive response operation*.

To enable a secure collaborating arena, while still protecting the individual actors' integrity, a bridge construction is used. This bridge acts as a gateway between the arena and an actors' internal information system and is owned and developed by the individual actor.

An Individual service is provided by an actor to the arena based on existing information within the actors' information system. In this case, the providing actor and the consuming actor may make an agreement of usage between themselves.

A Joint service is a service provided by one actor, but with an agreement with all actors in the arena on how information in this service should be treated. In this case, the information provided by this service resides with one actor in the collaborating arena.

A Composite service is a service which combines information from services provided by several actors. An example of this could be that one actor provides a composite service which contains information on all other actors' vehicle positions. An important part of the arena is the security mechanisms needed in order for the actors to trust that information from other actors is not compromised in any way and that the actors indeed are who they claim to be. It is vital for the function of the arena that security policies and security mechanisms are maintained based on a mutual agreement between the actors.

The IEAT Concept is build upon a set of key principles covering sovereignty, view on information, information exchange requirements, architecture, services, technology and security. These principles are further described in this chapter.

5.1 Key Principles

Sovereignty of collaborating parties

The sovereignty of the collaborating parties is fundamental, organisational right to use organic information systems and working methodology with various support tools shall in all situations be respected. The decision to publish information on the collaborating arena is the responsibility, and right, of each actor. Information content and possible restrictions will always be any actor's sovereign decision.

View on information

Information shall be regarded as an operations wide asset and not be exclusive to any single operational area or function, with exceptions for agreed confidentiality. Collaborating parties should avoid over-classification of information. Information should be provided as a published service.

Information Exchange

Agreements to facilitate Information Exchange shall exist for the *comprehensive response operation* and between the collaborating parties. The Agreements includes Information Exchange Models, Information Exchange Requirements, translations, semantic areas, instruments for data exchange, standardised data element catalogue, concepts and services for data translation.

Service Orientation

The IEAT concept uses Service Orientation as a principle. However, the term service is quite general and means different things in different contexts. For example, OASIS (organization) defines service as "a mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description."

In IEAT, services are technical services for information exchange following the tenets of the Service Oriented Architecture concept.

Architecture and Technology

Establishment of a consistent and understandable architecture should be supported by a common terminology and a common architecture description framework. The architecture description framework should support architectures both for the Mission perspective and the Technical perspective. The architecture description framework should cover at least following aspects of the architecture, Domain (Business), Information, Information Systems, Infrastructure, Security and Governance.

Open and accepted international standards, both civilian and military should be used. Bespoke and proprietary standards shall only be considered when it delivers significant higher value.

Commercially available solutions shall be considered in all areas, also taking life cycle cost into consideration. Bespoke development shall only be considered when the effects delivered provide considerable higher value.

Security principles

To achieve information exchange in a secure way using services, the IEAT concept defines a set of principles which guides the use of security functions:

- Service consumers and service providers must be able to identify themselves using a common method for authentication of users and services.
- There must be a common method to obtain integrity. A service consumer must be able to check that the data sent from another part is not changed by a third part.
- There must be a common method to guarantee the confidentiality of the information exchanged. This means that it should not be possible for any outsider to get access to the information that is exchanged.

5.2 Information Exchange

In order to meet operational needs for information exchange and to build a collaboration arena, supported by technical systems serving as operational nodes, a number of areas must be addressed;

- Information Exchange Requirement specifications
- Information Exchange Models within collaboration areas and their relation to international standards, domain Community Of Interest (COI) models, semantic structures etc
- Translation specifications and/or translation mechanisms
- Structure of information exchange facilities in the collaboration arena e.g. common data management services, translation services and bridges to external systems

5.2.1 Information Exchange models

When designing information exchange standards several different approaches may be applied:

- Model based
- Ontology based
- Message based

IEAT emphasises the model based approach but does not exclude that other approaches are included at a later point in time.

5.2.2 Translations

There may be a large number of translations between two information models. Each translation is based on thorough analysis and is documented in a translation specification together with estimates of information loss.

There are several principally different approaches to making translations between the models:

- manual model mapping, that is when two models are compared and decision are made at element level on how to map and/or translate to the other models. This is often the case

when the models to compare are documented according to different standards regarding ontological metadata notation, modelling style etc.

- rule based model mapping that is when two models are compared and mapped to each other based on formalized rules. This case requires common ontological metadata standards and the area is still in focus for ongoing research. Automated translation has the potential to be applied in runtime, thus increasing flexibility in information exchange.
- Standards message approach that is when a standardized message specification is mapped on to the models and to the concerned service interfaces. This approach is useful when a message standard is used and one or more of the models and/or the message standard is implicit rather than explicit regarding the information model.

The use of Translations in design of services is controlled by dedicated design rules.

5.2.3 Information objects

The construct of information objects, that is, set of data items contained and treated as a unit, are needed for several purposes in IEAT like security and information management.

Information may be managed at two levels of control:

- Information object, type/class level
- Information objects, instance level

When moved between systems an information object may be “carried” by several different requirements and one requirement may carry several different information object types and of course, instances of those types.

5.2.4 Formats

There are a number of domain formats, national formats and formats maintained by international standardisation groups. When implementing information exchange one or several different formats need to be used. Existing formats often include explicit or implicit information and data models, requirements and protocols for a subset of information in an IEAT collaboration arena. Thus, there is a need to be able to translate information according to IEAT standards to those of specific formats.

How to use specific formats in the design of IEAT collaboration arenas will be guided with designs rules and supported by Translations.

5.3 Architecture

The IEAT Concept outlines an architecture that enables a technical structure and technical means that provides a foundation for the collaboration arena in which information exchange among parties can take place. The architecture is described to a level that gives enough guidance to establish the collaboration arena based on existing systems and services or to develop new systems and services targeted for the collaboration arena.

The IEAT Concept also contains the elements needed to enable secure information sharing between technical systems, organisations and individuals.

The architecture is described by:

- Systems in terms of mission and/or technical capabilities.
- Governing aspects (design principles and rules) used to explain and develop architectural principles and structures in important areas of the architecture.
- Common terminology & definitions.
- Structure. How systems, aspects and terminology/definitions are organized and grouped.

5.3.1 Service Oriented Architecture

The Architecture of IEAT is Service Oriented. The aim of this is to achieve a loose coupling of services with underlying systems, whether it is mission or technical systems. So, instead of describing interaction directly between systems, the systems use services to interact with each other. By specifying a contract for information exchange, a service definition, the inside of a system can be replaced or modified without having to change other systems which interacts with it.

Services used or provided by technical systems should as far as possible be expressed in a common way and contain formal descriptions suitable for IT processing.
The Service description shall contain:

- The allowed service protocols (process) to be used for information exchange.
- The interfaces (or message types) that are used to exchange information between a service consumer and a service producer.
- The definition of the data types that are used in the interfaces (messages) and therefore are in the information exchange model.
- The properties that consumers can use to distinguish between different implementations of a service.

To enable systems to find and connect to each other, information about services shall be published and accessible for the collaborating parties' IT systems.

5.3.2 Information Technology based enablers needed to enable secure information sharing

To enable secure information sharing between technical systems and humans using Information Technology a set of core enablers are needed when establishing the collaboration arena. These are described below.

Service registry

The Service registry enables the technical systems to discover each other. The service registry is a vital part needed for enabling the loose coupling between systems since it provides functionality for the systems to find each other , with such registry the relationships between the systems does not need to be hard coded into the systems.

- Service Provider
  - provides services, i.e. functionality on the network

- publishes availability of Services through the Service registry

- Service Registry
  - provides support for publishing and locating services
  - like telephone yellow pages

- Service Consumer
  - locates required services via the Service Registry
  - binds to services via Service Provider

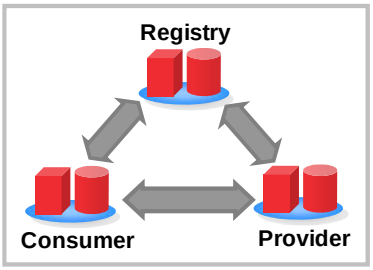

Figure 2: Service registry

Information discovery

Information discovery gives the possibility to discover information amongst the partners in the mission. Included in this is both a mechanism to crawl the information of the partners, just like search engines does, and also the possibility for the partners to publish selected information onto a central repository.

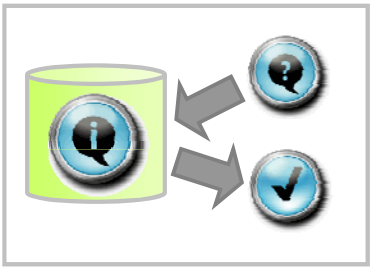
Figure 3: Information discovery

User registry

To be able to reduce the manual work needed to create users in all systems and create a transparency between the systems between the partners in the mission a federated user registry is needed. This, together with the security will give the users the feeling that it is one system they are using, not several different systems.

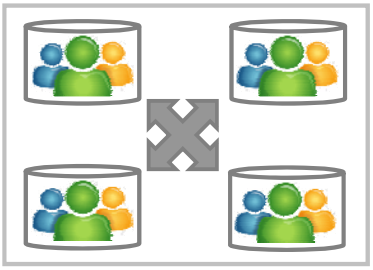
Figure 4: User registry

Collaboration services

In order to have information exchange between humans, collaboration services is a must. This enable users to send and receive messages by chat or e-mail, talk to each other and do video conferencing. Included in collaboration is also presence information which gives the ability to know if people are available or not.

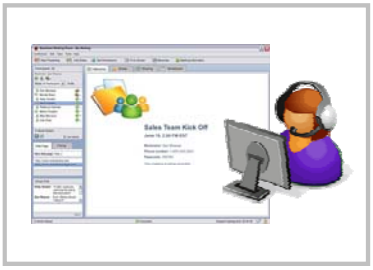
Figure 5: Collaboration services

Security services

Once discovery has been done, there must be a way to establish secure communication between the services in the technical system. The security services which enables this includes authentication services to verify that a user or a system really is who it says, authorization services to verify which things a user or system has access to, encryption services to enable secure transport of messages between systems.

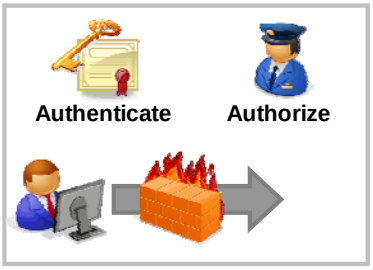

Figure 6: Security services

Management services

To be able to manage the technical systems in a consistent and federated form is a must in the type of distributed and ever changing environment that this type of system creates. The core of this is a monitoring capability which can monitor the availability and performance of all the systems. Another vital part is the ability to control how the technical system behaves by using policies or direct controlling actions.

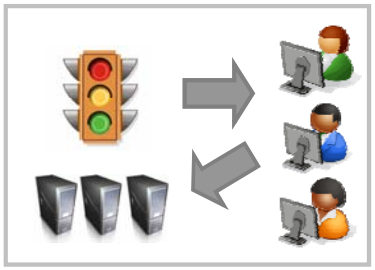

Figure 7: Management services

Mediation services

The mediation services are there to transport and transformation messages between different technical systems. The mediation service includes:

- Routing messages to the correct destination.
  This includes the ability to send messages asynchronously, i.e. that the sender and receiver does not need to be available at the same time and the ability to send messages to one or many destinations at the same time.
- Changing transport protocols of messages.
  This is the equivalent of changing transport modes, like changing from the train to the bus. The message is the same, but the transport differs.
- Transforming messages to other formats.
  This capability enables messages to be automatically translated between different information models. This is the same as an automatic language translator.

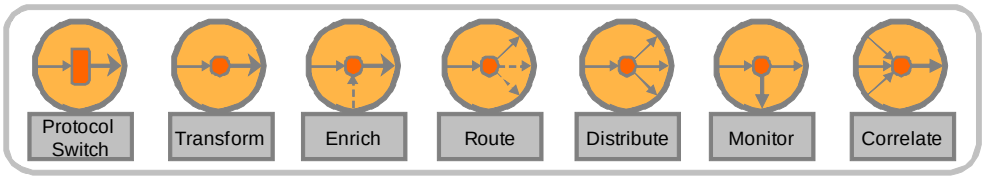

Figure 8: Mediation services

The summarized picture of elements needed to enable secure information sharing between technical systems and humans using Information Technology is illustrated in Figure 9.

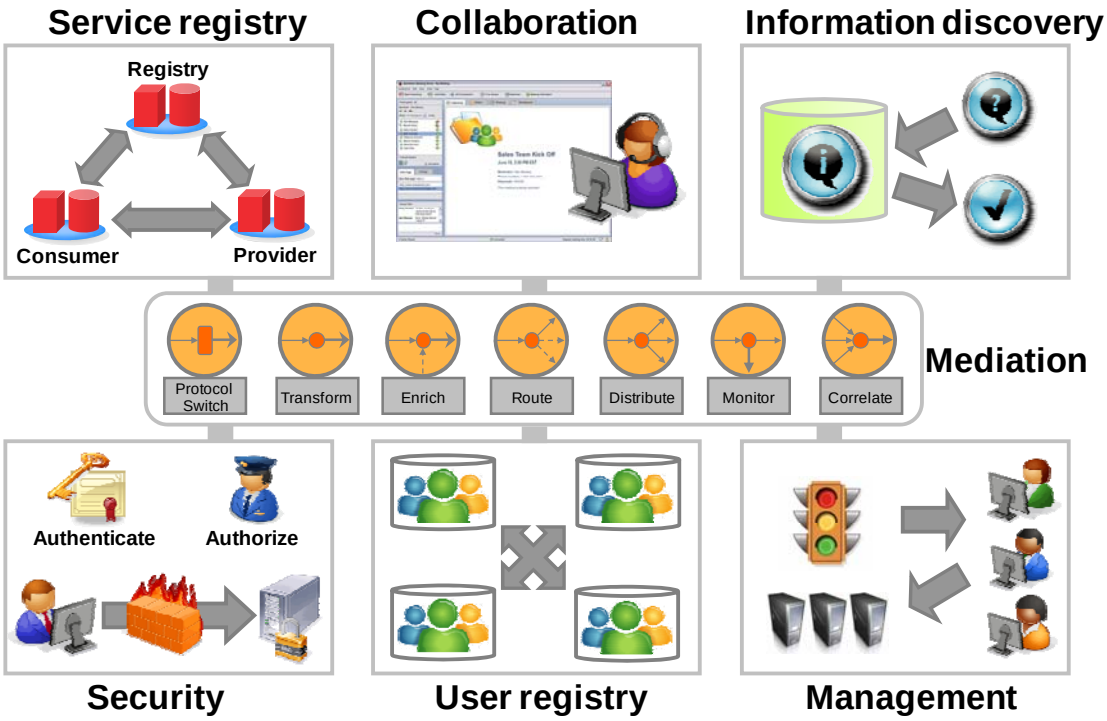

Figure 9: Information exchange architecture overview

5.3.3 Architecture description framework

In order for all parties to obtain a common "language" on how to describe their systems and the services they bring to the collaboration arena the IEAT Concept also covers an architecture description framework. The architecture description framework does not describe the architecture itself, but rather guides how the architecture shall be structured and what it should describe. An important aspect of the architectural description framework is to identify clear ownership of the different parts of the architecture.

The IEAT architecture description framework is based on the NATO Architectural Framework (NAF) version 2 which provides the rules, guidance, and product descriptions for developing, presenting and communicating architectures. As NAF version 3, the IEAT architecture description framework has been complemented with support for services.

The architecture description framework has three pillars (shown vertically in Figure 10: Architecture structuring principle) which have different purposes:

- The Technical pillar defines the technical systems and the division of these into groups.
- The Aspect pillar defines the common aspects applicable for the architecture.
- The Mission pillar defines the different missions.

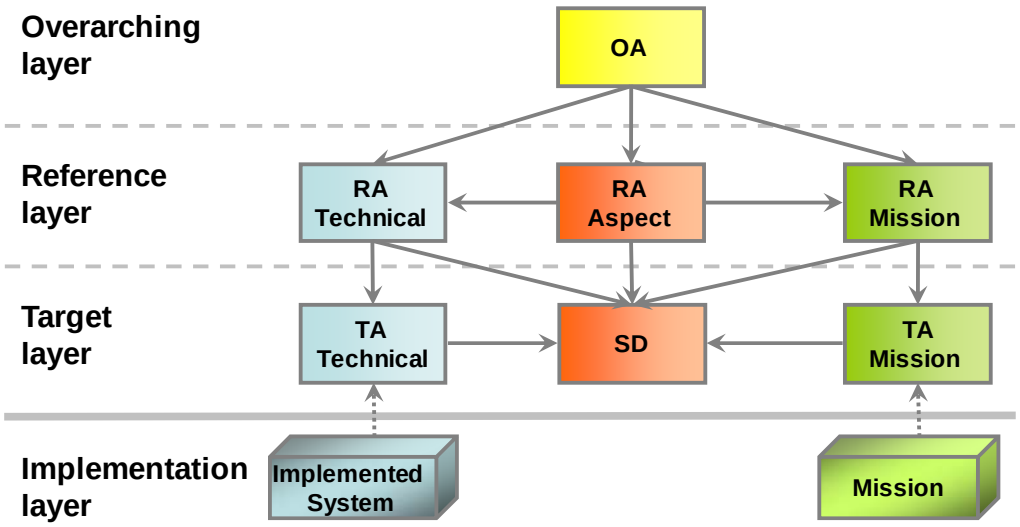

Figure 10: Architecture structuring principle

The architecture is also structured in a set of layers. These layers represent different levels of aggregation and time. They also have a hierarchical relationship which is used to govern the architectural structure.

The **Overarching Architecture (OA)** is used to identify areas of systems and aspects at highest level and sets the general principles and rules for all subordinate Reference Architectures (RAs) and Target Architectures (TAs). It is used to handle long term development and the definition of RAs.

Reference Architectures define and organize Target Architectures and define the need to develop reusable systems or reusable common behaviour in specific aspects, e.g. common security solutions.

RAs primary focus is on services, process and functionality and participating systems and establish strategic decisions regarding system technologies, stakeholder issues, product lines, etc.

Target Architectures are used to describe systems. TAs focuses on describing a systems outside and borders (black-box view) and the inside of the systems (white-box view) including their associated components, products and services.

The **Service Descriptions** are a key component of a Service Oriented Architecture. They are used to detach the functionality provided by a system (or services provided by an organizational unit) from the actual system. In this way it is possible to replace the system providing the service without changing the consumers of the service.

Service Descriptions includes information on how to interact with the service, what requirements a system must fulfil if it implements the service and what information model the services uses.

The Implementation layer describes the actual missions and technical systems. The systems in the Implementation layer implements the architecture described in the Target layer.

5.4 Security

The IEAT Concept focuses on the sharing of information between parties that don't necessarily have a prior and established relationship. This implies that trust to and reliability of the information shared must be dynamically handled.
Methods and mechanisms for identifying users and guaranteeing integrity of information objects are vital enablers for the concept to be feasible. A conceptual solution outline is presented below.

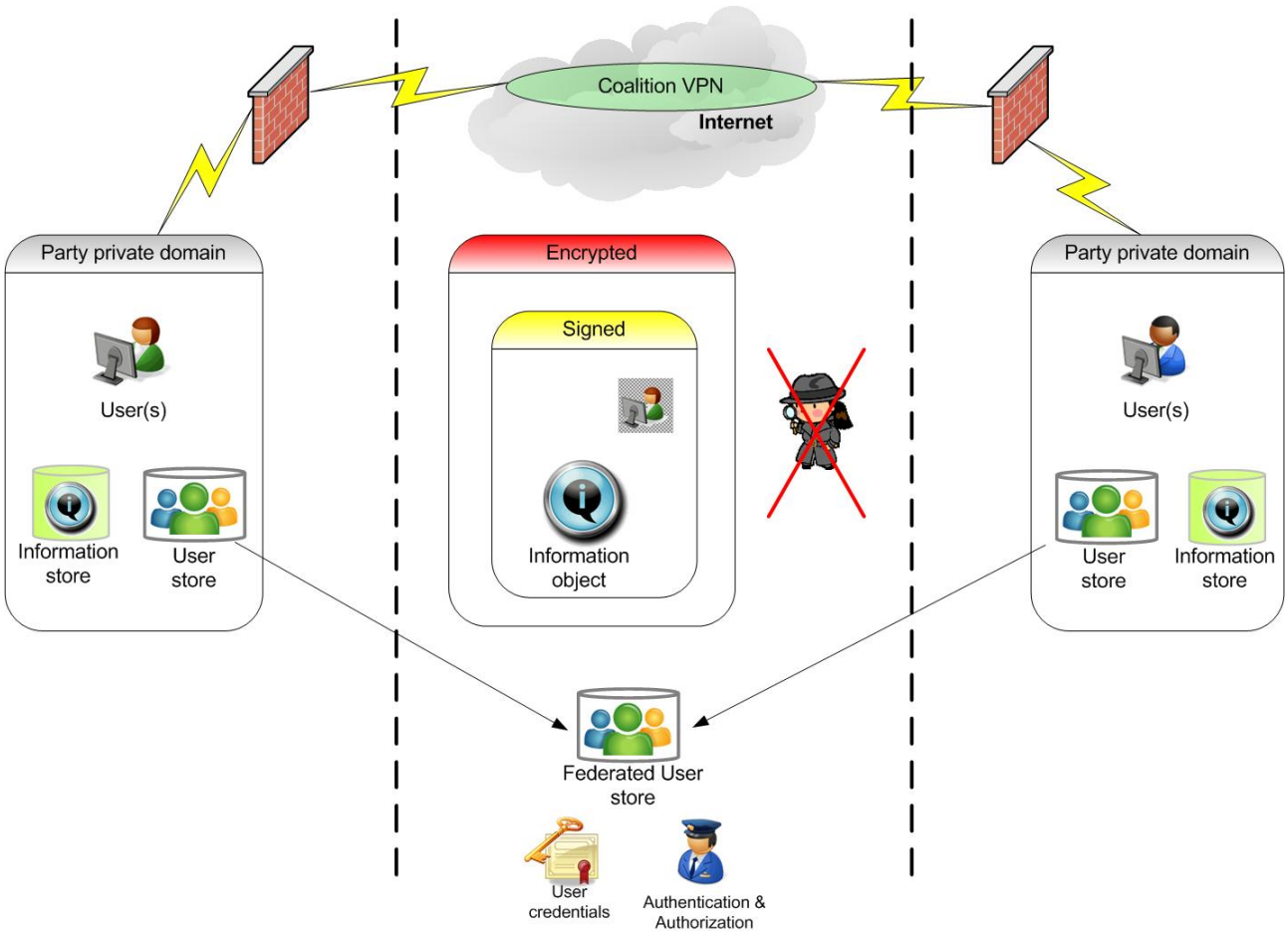

Figure 11: Conceptual security solution

This solution includes a key set of technologies to protect the information being shared on several different levels.

First, the transport is encrypted to make sure no one can listen on the network and pick up information. This is type of protection is very commonly used in the internet.

Secondly, messages can be protected by signatures in order to make sure they have not been read or altered during their journey across the collaboration arena. This is useful when messages are handled by another party than the intent receiver.

The technology also includes mechanisms to provide identity control (Authentication) and access control (Authorization). This enables the provider of a service to ensure that information is only given to those who can be trusted to handle it.

By utilizing a federated User store to perform authentication of users, it is possible for each participant in the Collaboration arena to manage their own user accounts (user credentials), thus minimizing the risk of loosing credentials and also minimizing user administration costs.

The objectives of having the security components as an integral part of the IEAT concept are described below:

Confidentiality	*to keep information secret for everybody but the intended users/roles/services*
Integrity	*to ensure that the information has not been manipulated*
Non-Repudiation	*to be able to prove who or what service is the origin of the information or action*
Identification/ Authentication	*to be able to identify and prove the identity of users and services*
Authorization/ Access Control	*to give the user/role/service access to information/services with the predefined/evaluated access level*
Availability	*to ensure the availability of information/services*
Privacy	*to ensure that personal information is not used in non sanctioned ways*
Safety	*to ensure the safety of people and environment when information technology is used in "physical" and logical operations*

Table 1: Objectives of security

6 Establishment and use of the IEAT Concept

The IEAT concept has been developed starting with the ideas in Revolutionary Military Affairs (RMA), Network Centric Warfare and Network Enabled Capabilities concepts. The ability and use of networked capabilities is still considered as having one of the greatest potentials for increasing combat effectiveness. The technique is already there, the biggest challenge is our ability to change our minds about the way we are thinking and using information.

Bearing this in our mind, it is necessary to see this chapter as qualified guesses based on a number of experiments and trials.

Formalised information exchange agreements are the basis for defining participating units and systems, regardless if the focus is on a national or an international operation. Consequently, a prerequisite for a functional IEAT Concept is that national preparations are made before setting up international units and systems. The national perspective is then brought into the planning of the multinational operation. When a crisis emerges, preparations between the actual participating parties need to continue. Planning for the actual operation must then also include definition of information exchange.

6.1 Understand, accept and change attitude

In order to establish understanding and acceptance it is necessary to address all challenges, described earlier in this document. In addition, understanding of the potential benefits of information sharing, gives motive for changes.

Experiments have shown that we tend to be prisoners of our heritage. We hesitate to share information with others even if the overall objectives will benefit from it. When confronted with scientific analyses, we easily agree that sharing information would have increased the effectiveness of the operation. Suspiciousness is jeopardizing our goals.

We do not believe that change of attitude will happen overnight. This is something that we gradually evolve over time when we force our self to get started.

To some extend there is an Internet analogy here. To understand the full potential of the concept it is necessary to get started and to gradually see how the increased effectiveness is coming.

6.2 Participation and acceptance of sharing information

In challenges 3.5 (Challenges lack of trust, mental block and organizational issues) we addressed problems related to our mental state of mind. We are hesitating to give away information to others, if we don’t see immediate personal gain of it.

Acceptance and full participating from the beginning from all actors are required for a successful implementation of IEAT. This is absolutely necessary. If one actor does not accept that we all gain from sharing information and do not participate, the IEAT concept and the effect of it will most likely fail. It is necessary to give this problem full attention in the coalition.

One way to approach this problem is to involve high rank officials in the process already from the beginning. With leaderships attention it is much easier on lower levels to maintain the necessary mental framework for success.

If we see early results from information sharing we will gradually increase the effectiveness and understand the long term benefits.

6.3 Establish the "physical" playground for information exchange

The technical challenge of implementing IEAT is most likely the easiest to solve. Civilian technology and civilian products are gradually implementing more and more functionality for information sharing in products. Still, we need to give technology full attention in the implementation phase and before.

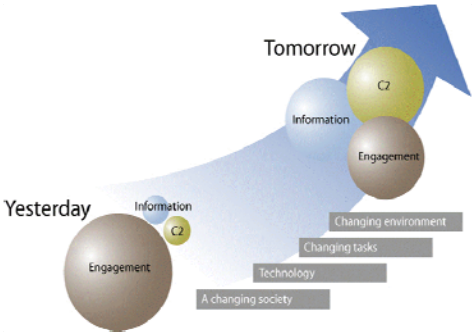

Figure 12: Increased effectiveness by sharing information

It is necessary to agree to a shared subset of interfaces needed for publishing and subscribing to information. Using commercially accepted and open standards and interfaces is a critical success factor for ensuring a good interoperability between the technical systems. To achieve this, it is important to drive and participate in standardization work, both in the military and civilian contexts.

We found it most likely that one nation needs to step forward in order to get the implementation and testing procedures starting.

It will be important not to start with to high expectation, gradually increased functionality will help the process going. Remember to keep a good balance between technology which gives user and business functionality and technical efforts which drive non-functional capabilities such as flexibility, security and scalability.

It is also important to have technical involvement during all stages of the lifecycle, starting with experiments to support concept development all the way through the actual operations. This will make sure that full advantage is taken of the technology and that the experiences can be shared between the different stages of the lifecycle.

6.4 Establish the "logical" playground for information exchange

When units become operational, more information agreements have to be signed. Military authorities have to sign agreements with necessary civilian authorities do necessary changes, train and act accordingly.

Please remember, it is not only a matter of receiving information, systems will most likely create information that other systems will benefit from. As stated earlier international information exchange

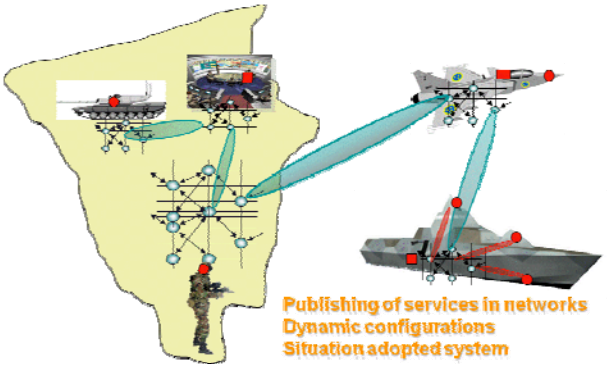

Figure 13: Published services in an IEAT environment

starts with formal agreements between states. It is therefore important to involve national legal authorities early in the process.

In an IEAT Concept based formation, participating parties need, during the initial planning process, based on information sharing agreements, sit together and define participating units, systems and subsystems. This activity defines requirements for necessary changes of systems and subsystems. Here we create the possibility of using sensors from one partner together with weapons from another partner and vice versa. We will also see where we could optimize and how we will be able to create necessary overlapping functions.

One part of the day-to-day work is to continue to conduct IEAT preparations, the more agreements and decisions on information sharing that can be made, time for preparations minimizes when operation starts.

As soon as necessary system changes has been made it will be necessary to start integrate our systems and start validate our units, both nationally and together in coalitions.

6.5 Before and during an international operation

Information to share and requirements on information need to be specified. Before action, commanders need to configure systems so that participating units will have a common operational picture to ensure success of the mission.

By building the system according to IEAT and using agreed upon standards for information exchange it is possible to orchestrate the information even during an operation. Changes could be made and tested within minutes and hours rather than within months. This could be achieved by subscribing to new information flow and by reconfigure the operational picture on the fly. This will highly increase the effectiveness of the operation.

Evaluated results from planning and mission shall immediately be fed back to our commanders in order to support future success.

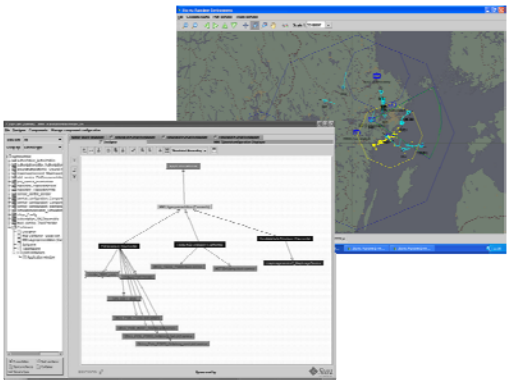

Figure 13: Situation adopted systems

6.6 Feeding back to the bigger loop, developing the IEAT concept

Agreements and other preparations made for an operation must be fed back to the routine activities for the participating parties, to be included as preparations for a coming future operation. It also has to be fed back to other planed multinational operations when appropriate.

This will include new requirements for systems at all levels.

Routine discussions between nations and parties must also include preparations and methods for effective information sharing.